

AI ve veřejné správě v provozu

Přínos. Odpovědnost. Důkaz.

AI přináší hodnotu až ve chvíli, kdy ji umíme bezpečně provozovat — a doložit, že zavedená opatření skutečně fungují.



AI v provozu není model. Je to řízená služba.



PŘÍNOS

Adoptovat

Vybrat konkrétní agendu, uživatele a výsledek, který lze sledovat. Ne „AI pro AI“, ale jasný provozní přínos.



ODPOVĚDNOST

Provozovat

Určit povolené zdroje, roli člověka, vlastníka služby, cílovou architekturu a pravidla celého životního cyklu.



DŮKAZ

Kontrolovat

Doložit zdroje, zásahy kontrol, auditní stopu a výsledky průběžných testů — nejen existenci směrnice.



Stejný rámec použijeme na dvou reálných příkladech Finanční správy ČR.

Nejdřív přínos a odpovědnost. Teprve potom model, infrastruktura a produkt.

IrčA: interní AI asistentka Finanční správy ČR

Podpora zaměstnanců při práci s IAŘ, metodikami a interními dokumenty



PŘÍNOS

Rychlejší orientace a dohledání relevantních informací



ODPOVĚDNOST

Odpovědi vycházejí pouze z interních zdrojů



DŮKAZ

Transparentní citace, auditovatelnost a lidský dohled

AI Pomoc s Daněmi: AI připraví, občan potvrzuje

Koncept předvyplněného daňového přiznání z podkladů dodaných občanem



 **Důležitý princip: AI pomáhá s přípravou podání, ale finální rozhodnutí vždy zůstává na člověku.**



PŘÍNOS

Zjednodušení přípravy podání



ODPOVĚDNOST

Finální potvrzení a rozhodnutí zůstává na občanovi



DŮKAZ

Kontrola a validace údajů před finálním potvrzením

Z pilotu do provozu: pět rozhodnutí před prvním produkčním promptem



Teprve po těchto rozhodnutích vybíráme model, infrastrukturu a technologický stack.

Kde AI provozovat? Rozhoduje agenda, ne preference dodavatele.



citlivost a suverenita dat



výkon a provozní stabilita



regulace, audit a
governance



predikovatelnost nákladů



Cloud

- ✓ méně citlivé scénáře
- ✓ rychlé škálování
- ✓ spravované modely a služby

Výhoda: rychlost a pružnost



Hybrid

- ✓ citlivá data a core AI lokálně
- ✓ méně kritické scénáře v cloudu
- ✓ společná kontrolní vrstva

Častý výsledek pro veřejnou správu



On-prem / SPCSS

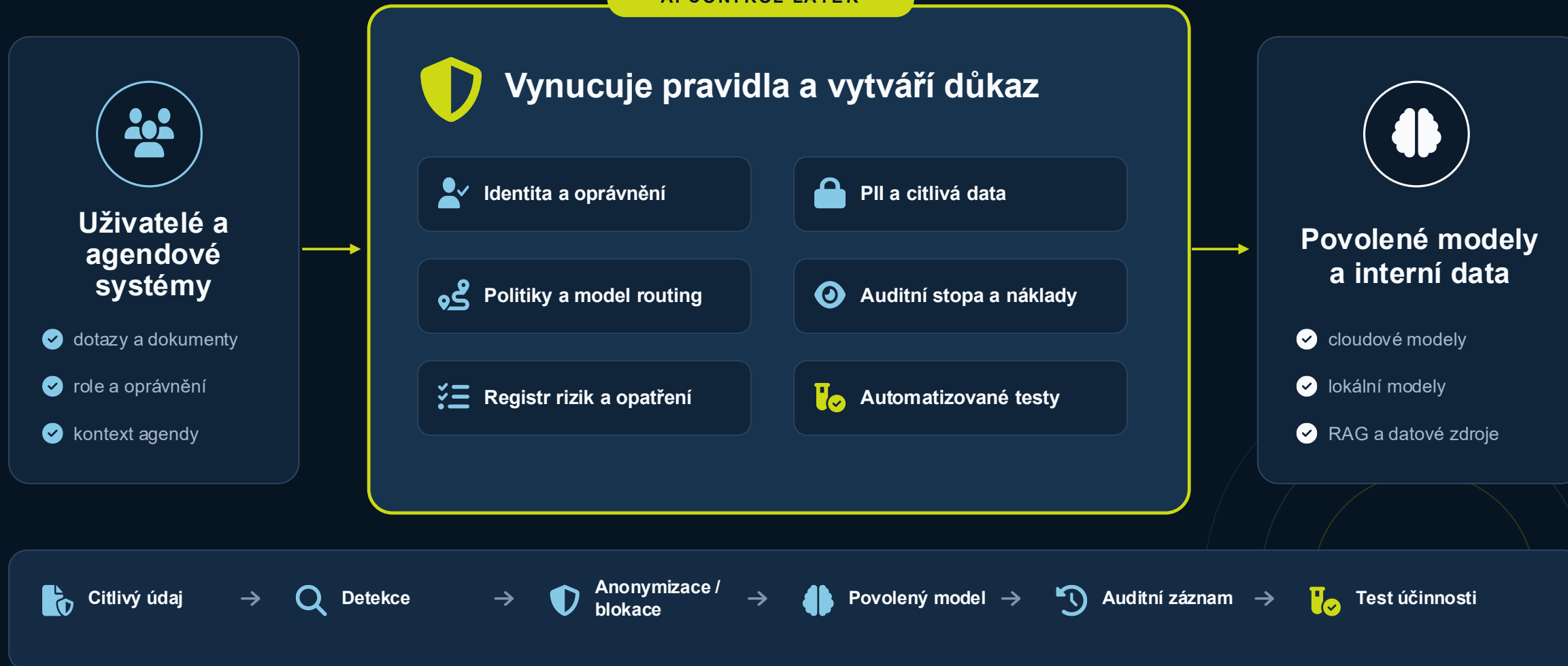
- ✓ vysoká citlivost a suverenita
- ✓ izolovaný nebo řízený provoz
- ✓ vyšší kontrola nad životním cyklem

Výhoda: kontrola a stabilita

Volba platformy je výstupem posouzení use-casu — nikoli výchozím dogmatem.

Kontrola není směrnice. Musí fungovat za běhu.

AI CONTROL LAYER



Datera tuto vrstvu realizuje mimo jiné prostřednictvím platformy **regul.ai**

Od AI nápadu k řízené provozní službě



ADOPTOVAT

- ✓ portfolio use-casů
- ✓ posouzení přínosu a rizik
- ✓ roadmapa pilot → produkce



PROVOZOVAT

- ✓ cílová architektura
- ✓ cloud · hybrid · on-prem
- ✓ integrace a provozní model



KONTROLOVAT

- ✓ pravidla a kontrolní vrstva
- ✓ registr rizik a testování
- ✓ auditní a provozní důkaz

 **Přineste jednu konkrétní agendu. Společně navrhujeme první bezpečný a měřitelný krok.**

ReguAudit AI: tři komponenty kontrolní a důkazní vrstvy



KOMPONENTA

Gateway

Runtime vrstva mezi aplikací a modelem: detekce a anonymizace PII, vynucování politik, směřování na povolené modely a auditní stopa.



KOMPONENTA

AI Risk Registry

Centrální katalog rizik, vlastníků, opatření a stavu nápravy. Udržuje provozní a compliance kontext jednotlivých AI služeb.



KOMPONENTA

Probe Runner

Aktivní testování odolnosti AI rozhraní a měření účinnosti ochranných filtrů. Vytváří průběžný důkaz, že opatření fungují.

Gateway vynucuje. Registry řídí. Probe Runner ověřuje.

AI Act: bezpečnost nestačí mít. Musí fungovat.

„Bezpečnostní pás“ musí být zapnutý – a při nárazu udržet.

DNES

Bezpečná AI landing zone



Azure AI landing zone
podle potřeb úřadu



datová suverenita
a řízení přístupu



izolace AI aplikací
a provozních prostředí



auditovatelnost jako
součást návrhu



AI Act readiness
know-how

LANDING ZONE
ZABEZPEČENO



PŘÍSTUP
POVOLEN
AUDIT



VŠE POD
KONTROLOU!

CHRÁNĚNO. AUDITOVÁNO.
POD KONTROLOU.

AI

BEZPEČNOSTNÍ

PÁS ZAPNUTÝ

CVAK!

PRASK!

BUDUJEME

Automatizovaná compliance AI aplikací



kontrola vůči
OWASP LLM Top 10



důkazy shody pro
AI Act / NIS2 / DORA



kontrola: přístupy,
filtry, logy, klíče



ověření, zda se ochrany
skutečně používají

DŮKAZY & LOGY

2024-05-20 10:15:21	ACCESS	OK
2024-05-20 10:15:22	FILTER	OK
2024-05-20 10:15:23	LOG	OK
2024-05-20 10:15:24	KEY	OK

PROOF OF
COMPLIANCE



OVĚŘENO!
OCHRANY FUNGUJÍ!

VÝSTUP PRO ZÁKAZNÍKA



Gap analýza



skóre
připravenosti



auditní
stopa



doporučení
ke zlepšení